



## ***Tecnologia - Phishing: l'era nuova in cui fidarsi è diventato un rischio (ma puoi ancora difenderti)***

**Roma - 02 lug 2025 (Prima Pagina News) Il phishing è diventato subdolo e personalizzato (email, SMS, QR code), sfruttando anche l'IA per clonare voci o scrivere messaggi credibili.**

Una volta bastava un'email piena di errori grammaticali e un link visibilmente insolito per capire che si trattava di una truffa. Oggi non è più così semplice. Il phishing, ovvero l'inganno informatico più diffuso in assoluto, è entrato in una nuova fase: più smart, più silenziosa, e molto più difficile da individuare. E purtroppo funziona: milioni di utenti e aziende cadono vittima ogni anno, spesso senza nemmeno accorgersene. Se sei convinto che "io non ci cascherei mai", sappi che è proprio questo il punto: oggi ogni attacco di phishing è progettato per non essere rilevato dai nostri radar. Il phishing oggi: meno superficialità, più astuzia. Nel 2025, il phishing non assomiglia più alla mail di un sedicente principe africano o a un improbabile comunicato bancario scritto male. Oggi può arrivare da quello che sembra il tuo capo, il tuo fornitore, il tuo cloud aziendale. E magari anche con un allegato PDF. Secondo il Phishing Trends Report 2025, il 64% delle aziende ha subito attacchi di Business Email Compromise (BEC) ovvero compromissione di account email aziendali, in cui i criminali fingono di essere dirigenti interni per farsi autorizzare bonifici o accessi. In media, ogni colpo è costato 150.000 dollari. E non ci sono solo le email. Il phishing adesso parla tutte le "lingue digitali": ? Spear phishing: email personalizzate basate su info reali, come il tuo ruolo o la tua azienda. ? Smishing: messaggi SMS che sembrano provenire da interlocutori affidabili, come corrieri o banche. ? Vishing: telefonate false da finti operatori. ? Quishing: QR code malevoli stampati su cartelloni, biglietti da visita o lasciati "casualmente" in giro. ? Phishing potenziato dall'intelligenza artificiale: messaggi scritti (bene) da LLM (Large Language Models come ChatGPT), magari con una voce clonata che ti chiama e ti chiede di "verificare i dati". Sì, ormai i truffatori usano l'intelligenza artificiale. E spesso la usano meglio di noi. AI e phishing: un'unione pericolosa. Anche se nel 2024 solo tra lo 0,7% e il 4,7% delle email phishing rilevate era scritta da AI, il potenziale è enorme. Soprattutto perché questi strumenti sono capaci di replicare tono, struttura e contenuti di messaggi reali. Il rischio cresce ogni giorno. Allo stesso tempo, il 90% dei siti phishing usa il protocollo HTTPS, quindi anche il "lucchetto sicuro" non è più garanzia di sicurezza. I brand più imitati (per farti abbassare la guardia) I truffatori usano nomi che conosci: Microsoft, DocuSign, il tuo team HR. Le email più cliccate? Quelle che dicono "il tuo account sta per scadere" o "firma urgente il documento in allegato". Aggiungi un logo ben fatto, una frase in apparenza neutra, e il gioco è fatto. Quanto è diffuso il problema? I dati più aggiornati provengono dagli Stati Uniti e ci dicono che, ogni anno, un'azienda da 1.000 dipendenti subisce circa 2.300 attacchi, con circa 466 clic reali. Con programmi formativi avanzati si può ridurre questa



cifra ma servono costanza, pratica e... attenzione umana. Come riconoscere ed evitare il phishing Non serve essere un hacker per difendersi. Bastano alcune abitudini sane: ? Controlla bene il mittente: anche se il nome è corretto, guarda l'indirizzo email completo. ? Verifica i link: passaci sopra con il mouse e guarda dove portano davvero. ? Non cliccare su allegati sospetti, specie se non ti aspettavi comunicazioni di questo tipo. ? Attiva la verifica in due passaggi (2FA) se possibile. ? Aggiorna browser, antivirus e sistema operativo. ? Ascolta il tuo istinto: se qualcosa ti sembra "strano", fai tutti gli approfondimenti del caso. Il phishing è un attacco psicologico prima ancora che tecnico. Fa leva su fretta, fiducia e abitudine. Ma con la giusta attenzione, strumenti tecnologici adeguati e una formazione di qualità, possiamo passare da anello debole a prima linea difensiva.

*(Prima Pagina News) Mercoledì 02 Luglio 2025*